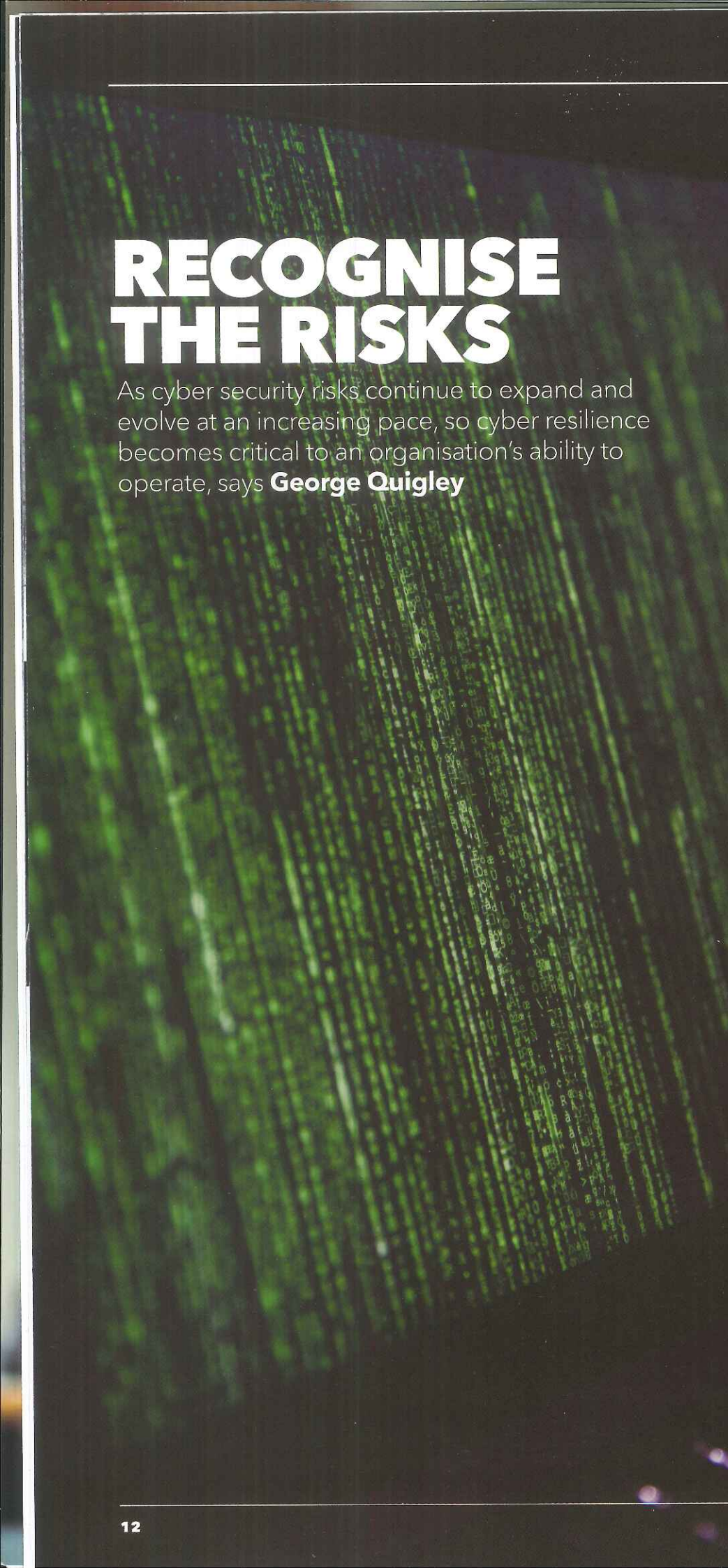

RECOGNISE THE RISKS

As cyber security risks continue to expand and evolve at an increasing pace, so cyber resilience becomes critical to an organisation's ability to operate, says **George Quigley**

Technology, in the context of a wider business, is an enabler that provides business advantage. A cyber risk management strategy, which effectively quantifies, qualifies and mitigates your technology risks, when properly aligned to your business strategy, will sustainably protect your business in a cost-effective, pragmatic and practical way. But how do you achieve cyber resilience?

BACKGROUND

While General Data Protection Regulation (GDPR) was headline news in 2018, the EU directive on the security of networks and information systems (known as the NIS Directive) was also transposed into UK law. This means that organisations in critical sectors (water, energy, health, transport and digital service providers) have to implement robust levels of cyber resilience, an indication of how seriously governments are taking this issue.

Although cyber resilience is a relatively new concept, it has its foundations in the past. It comprises cyber security, business continuity and operational resilience and aims to defend against cyber threats, enabling organisations to successfully recover following an attack.

FOUNDATIONS

Over the years, many organisations have had some form of disaster recovery plan in place, should important data be lost or IT systems fail. The same cannot be said for business continuity plans.

In fact, there are many examples where companies have been unable to continue operating effectively following system failure, even when those systems were back up and running at a disaster recovery site in a relatively short space of time. The IT team had translated what the business need was but the wider business was not engaged in the process, as they saw it as a technology problem, not a business issue.

A consideration of risk is needed in order to avoid this scenario. Cyber risk, as defined by the Institute of Risk Management, is the risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its IT systems.

APPROACH

To achieve robust and sustainable cyber resilience, a structured approach to the

consideration of risk is called for. A fast and effective approach that we have implemented involves four key steps:

1. **Business assessment.**
2. **Governance and oversight.**
3. **Risk management framework.**
4. **Incident response and recovery.**

BUSINESS ASSESSMENT

While you understand your business and how it operates, to what extent do you understand your use of systems and data, and how they drive value?

Do you know what your prized technology assets are and do you understand the interaction they have with other systems and data?

To what extent have you outsourced your infrastructure to third parties and do you understand the contractual obligations and liabilities that are placed on both parties?

A detailed assessment will allow you to build a clear picture of your technology and data assets, assess the economic impact of a cyber incident and provide the foundation for considering your governance and oversight mechanisms.

Throughout this assessment, keep in mind the three key elements of cyber security, namely confidentiality, integrity and availability. In particular, consider the implications of the regulatory environment, including the potential impact of GDPR.

GOVERNANCE AND OVERSIGHT

The next thing to consider is how well your governance framework and your approach to the management of risk deals with cyber risk. One of the issues that businesses often find particularly challenging is understanding the financial impact of an incident or breach. Businesses often ask if they are spending too much or too little on cyber security, on business continuity or on resilience.

The initial business assessment allows you to understand the likely financial impact of a cyber incident more fully. It helps you to make a better assessment of your risk appetite, which may be different for different elements of your business. Budgets can then be allocated accordingly. The aim would be to align the cyber risk strategy to the business strategy.Governance issues that should be resolved include:

Using your business asessment, you can ask a number of key questions designed to check whether your management of cyber risk is complete

- Who is responsible for cyber risk at a senior level?
- Who is managing those risks?
- How are they being reported to the board?
- Have you considered all legal and regulatory risks?

Your governance arrangements, combined with your business assessment, provide the basis for evaluating your risk management practices.

RISK MANAGEMENT FRAMEWORK

Most businesses operate a risk management framework, albeit with varying levels of formality. How your risk management framework deals with cyber risk is your next consideration.

Using your business assessment, you can ask a number of key questions designed to check whether your management of cyber risk is complete and operates in such a way as to bring the residual risk in line with your risk appetite. These questions include the following:

- Have you identified all of the key cyber risks you are exposed to?
- Are you still content with your assessment of the impact and likelihood of those risks occurring?
- Are you still happy with the way those risks have been addressed (treat/transfer/avoid/accept)?
- For those we are treating, do the controls that we have noted appear to be sufficient?
- Do you need the controls you have?
- Could you achieve the same aim with more efficient controls?
- Do you need additional controls?

This process should help identify any gaps, which can then be dealt with in order to appropriately address the risk.

INCIDENT RESPONSE AND RECOVERY

What we haven't yet assessed is what happens when you have a control or other failure that leads to a system failure. For that you need to consider your incident response and recovery plans, and how they align to your business continuity and other resilience plans.

You need to assess how robust your incident response plans are:

- Are they based on risk and prioritised appropriately?
- How would you identify an incident?
- Do your plans allow you to recover in a timely manner?
- How have they been aligned to your business continuity strategy?

Once completed these plans should be tested in order to assess how effective they are. Key learning opportunities include understanding what tensions were encountered during the test and what gaps were identified. Your plans should also be revisited regularly to ensure they evolve in line with changes to the business and to address new threats as they emerge.

There may be instances where you identify gaps that you cannot close. In these instances you need to consider to what extent you need to update your communication plans so that you can inform and reassure your clients, regulators and wider stakeholders.

Taking a structured, risk-based approach to cyber resilience, aligned to your business strategy, will enable you to take practical and pragmatic steps to protect your business in a cost-effective way.

The approach outlined above can identify cost savings that can make the exercise cost-neutral or, in some cases, positive while achieving the aim of understanding and reducing your risk of a cyber attack. ●

George Quigley, cyber risk consultant with foulkon.com and KPMG ex-partner, provides insights into cyber resilience